

Beveilig uw organisatie

10 tips voor betere cybersecurity

ABN·AMRO

Voorwoord

Een gehackt e-mailaccount, een vervalste factuur of bestanden die niet meer openen; digitale problemen kunnen uw bedrijf stilzetten. Ze kunnen ook leiden tot verlies van gegevens, financiële schade en minder vertrouwen bij klanten. Deze brochure helpt u om uw bedrijf beter te beschermen en u voor te bereiden op een incident.

Cybersecurity richt zich vooral op het voorkomen van incidenten, met maatregelen die systemen, gegevens en processen tegen digitale aanvallen beschermen. Cyberweerbaarheid betekent ook dat u problemen herkent, de gevolgen beperkt en uw werk kunt hervatten. Geen enkele maatregel biedt volledige bescherming. Daarom zijn voorkomen én voorbereiden belangrijk.

U hoeft niet alles tegelijk te regelen en u heeft niet voor iedere maatregel een eigen IT-afdeling nodig. Begin met veilig inloggen, beperkte toegangsrechten, software-updates en betrouwbare back-ups. Spreek duidelijk af wat u zelf doet en waarvoor uw IT-leverancier verantwoordelijk is.

Deze brochure bevat tien tips. Deze tips hebben steeds dezelfde opbouw: wat u doet, waarom dat belangrijk is, wat u zelf kunt regelen en wat u aan uw IT-leverancier vraagt. De checklist achterin heeft dezelfde volgorde. Die bevat basismaatregelen, onderwerpen om te bespreken met uw leverancier en aanvullende maatregelen die afhangen van uw risico's.

Gebruik de checklist om vast te leggen wat al geregeld is, wie de overige acties oppakt en wanneer. Kijk de afspraken regelmatig na. Zo maakt u digitale veiligheid onderdeel van uw dagelijkse bedrijfsvoering.

1. Beveilig het inloggen

Wat doet u? Gebruik voor ieder account een sterk, uniek wachtwoord en beveilig het inloggen met een extra controle. Deze extra controle heet multifactorauthenticatie, vaak afgekort tot MFA.

Waarom is dit belangrijk? Met gestolen inloggegevens kan een aanvaller toegang krijgen tot uw e-mail, administratie of klantgegevens. Een uniek wachtwoord voorkomt dat een gelekt wachtwoord ook op andere accounts werkt. Een extra inlogcontrole verkleint het risico op misbruik, maar sluit dat niet volledig uit.

Wat kunt u zelf doen? Gebruik een wachtwoordkluis om sterke wachtwoorden te maken en veilig te bewaren. Beveilig de kluis met een sterk hoofdwachtwoord en een extra controle. Deel wachtwoorden, eenmalige codes en andere verificatiecodes nooit met anderen.

Controleer of de extra inlogcontrole actief is voor uw zakelijke e-mail, bedrijfsapplicaties en bankomgeving.

Wat vraagt u aan uw IT-leverancier? ‘Welke accounts hebben nog geen extra inlogcontrole? Welke methode past bij ons bedrijf? Kunnen we passkeys gebruiken?’

Passkeys zijn gebruiksvriendelijk en beter bestand tegen phishing en wachtwoorddiefstal dan traditionele wachtwoorden. Bij passkeys is altijd een fysieke actie nodig die alleen door de gebruiker zelf kan worden uitgevoerd.

Vraag ook hoe u veilig toegang herstelt als een medewerker een telefoon of passkey kwijtraakt. Beoordeel de gekozen inlogmethode en de herstelprocedure samen; ga niet uit van volledige bescherming door één techniek.

2. Geef alleen toegang die nodig is

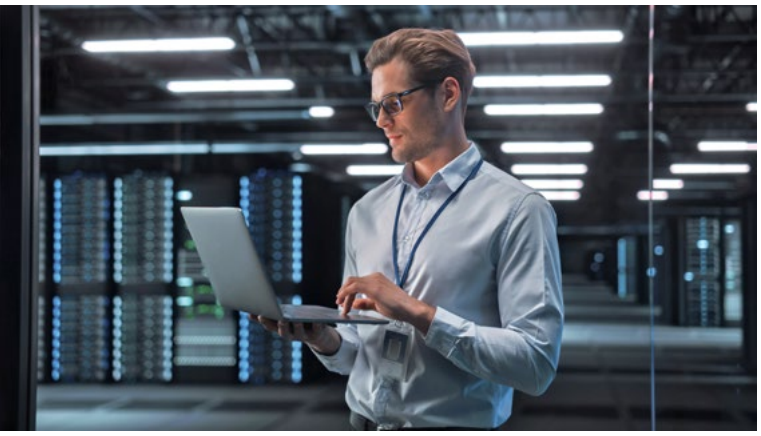
Wat doet u? Geef medewerkers en externe dienstverleners alleen toegang tot de gegevens en systemen die zij voor hun werk nodig hebben. Een sales medewerker hoeft bijvoorbeeld niet automatisch toegang te hebben tot de personeelsadministratie.

Waarom is dit belangrijk? Als een account wordt overgenomen, bepalen de toegangsrechten mede wat een aanvaller kan doen. Beperkte rechten helpen de mogelijke schade te verkleinen.

Wat kunt u zelf doen? Houd bij wie toegang heeft tot welke systemen. Controleer dit regelmatig en pas rechten aan als werkzaamheden veranderen of iemand vertrekt. Laat medewerkers geen inloggegevens of toegangspassen delen.

Spreek af wie nieuwe software mag goedkeuren en installeren. Beheerdersrechten (administratorrechten) geven iemand de mogelijkheid om belangrijke instellingen te wijzigen en software te installeren. Geef deze rechten niet standaard aan iedereen.

Wat vraagt u aan uw IT-leverancier? ‘Wie heeft beheerdersrechten? Hoe beperken we die? Wie controleert de toegang van medewerkers, onze boekhouder en andere leveranciers, en wie trekt onnodige rechten in?’ Leg de afspraken vast.



3. Houd software en apparaten up-to-date

Wat doet u? Installeer beveiligingsupdates tijdig. Doe dit niet alleen voor computers, maar ook voor alle bedrijfsapplicaties, printers, routers en andere apparaten met software.

Waarom is dit belangrijk? Software kan fouten bevatten die aanvallers misbruiken. Beveiligingsupdates herstellen zulke kwetsbaarheden. Uitstel laat bekende beveiligingslekken langer openstaan. Nieuwe, krachtige AI-technologie maakt het opsporen van fouten veel sneller. Aanvallers gebruiken deze nieuwe technologie om aanvalsscenario's en malware te ontwikkelen. Hierdoor wordt de periode tussen het ontdekken van een fout en het misbruiken ervan steeds korter.

Wat kunt u zelf doen? Houd een overzicht bij van uw apparaten, systemen, applicaties en accounts. Spreek per onderdeel af wie updates verzorgt. Vervang verouderde systemen die geen beveiligingsupdates meer krijgen.

Wat vraagt u aan uw IT-leverancier? 'Welke onderdelen werken jullie bij en welke moet ik zelf regelen? Hoe snel installeren jullie belangrijke beveiligingsupdates? Hoe controleren jullie of de update is gelukt en ons werk nog goed kan doorgaan?'

Wilt u een oude laptop weggeven of afvoeren? Laat uw IT-leverancier zorgen dat bedrijfsgegevens veilig worden gewist en controleer hoe dat is gedaan. Ga er niet zonder meer van uit dat alleen het opnieuw installeren van het besturingssysteem voldoende is.

4. Maak en test back-ups

Wat doet u? Maak regelmatig back-ups van de gegevens die uw bedrijf nodig heeft. Denk aan uw administratie, klantgegevens, procesinformatie en voorraadgegevens. Bewaar minimaal één recente kopie offline, buiten bereik van uw bedrijfsnetwerk.

Waarom is dit belangrijk? Een digitale aanval, brand, waterschade of een menselijke fout kan gegevens onbruikbaar maken. Een recente back-up helpt u om verloren informatie terug te zetten en uw werkzaamheden te hervatten.

Wat kunt u zelf doen? Bepaal welke gegevens u niet kunt missen en controleer of die in de back-up zitten. Spreek af wie controleert of de back-ups worden gemaakt.

Wat vraagt u aan uw IT-leverancier? 'Hoe vaak maken jullie back-ups? Waar staat de offline kopie? Wanneer hebben jullie voor het laatst getest of alles kan worden teruggezet?' Laat bij een test en na herstel controleren of de gegevens volledig, onbeschadigd en bruikbaar zijn. Leg de resultaten en eventuele problemen vast.

5. Bescherm apparaten en verbindingen

Wat doet u? Gebruik antivirussoftware en firewalls. Antivirussoftware helpt schadelijke software te herkennen, te blokkeren en te verwijderen. Een firewall bepaalt op basis van ingestelde regels welke netwerkverbindingen zijn toegestaan.

Waarom is dit belangrijk? Schadelijke software kan gegevens stelen, bestanden versleutelen of wissen. Antivirussoftware en firewalls zorgen voor een sterke basisbeveiliging. Ze verminderen het risico op datalekken, financiële schade, reputatieschade en verstoring van bedrijfsprocessen. Hoewel geen enkele beveiligingsmaatregel volledige bescherming biedt, verkleinen deze technische oplossingen de kans op cyberaanvallen aanzienlijk.

Wat kunt u zelf doen? Controleer of de beveiliging actief is en houd deze up-to-date. Vergrendel computers en mobiele apparaten met een pincode, wachtwoord of biometrische controle. Versleutel gevoelige gegevens op apparaten en tijdens verzending om ze onleesbaar te maken voor derden.

Wat vraagt u aan uw IT-leverancier? 'Zijn alle zakelijke apparaten zoals printers en routers beschermd? Wie beheert de firewall en volgt beveiligingsmeldingen op? Is versleuteling geregeld voor onze apparaten en gevoelige gegevens?' Laat ook beoordelen of aanvullende beveiliging nodig is om verdacht gedrag op apparaten te herkennen.

6. Maak beveiligingsafspraken met leveranciers

Wat doet u? Bespreek digitale veiligheid met leveranciers die toegang hebben tot uw gegevens of systemen. Denk aan uw IT-dienstverlener, webshopbeheerder en aanbieder van online boekhoudsoftware.

Waarom is dit belangrijk? Uw bedrijf is ook afhankelijk van de beveiliging van diensten die u inkoopt. Een probleem bij een leverancier kan uw gegevens of bedrijfsvoering raken, zeker als systemen automatisch informatie uitwisselen.

Wat kunt u zelf doen? Houd bij welke leveranciers toegang hebben en welke diensten belangrijk zijn voor uw werk. Leg afspraken over beveiliging en het melden van incidenten vast in contracten. Noteer uw bevindingen en controleer de afspraken regelmatig. Controleer of uw bedrijf onder de Cyberbeveiligingswet valt en welke verplichtingen dan gelden.

Wat vraagt u aan uw leveranciers? 'Hoe beveiligen jullie onze gegevens en jullie toegang? Welke verbeteringen voeren jullie door? Wie waarschuwt mij bij een incident? Hebben jullie een noodplan en is dat getest?' Bespreek ook hoe uw bedrijf verder kan als de dienst tijdelijk uitvalt.

7. Herken misleiding en meld verdachte situaties

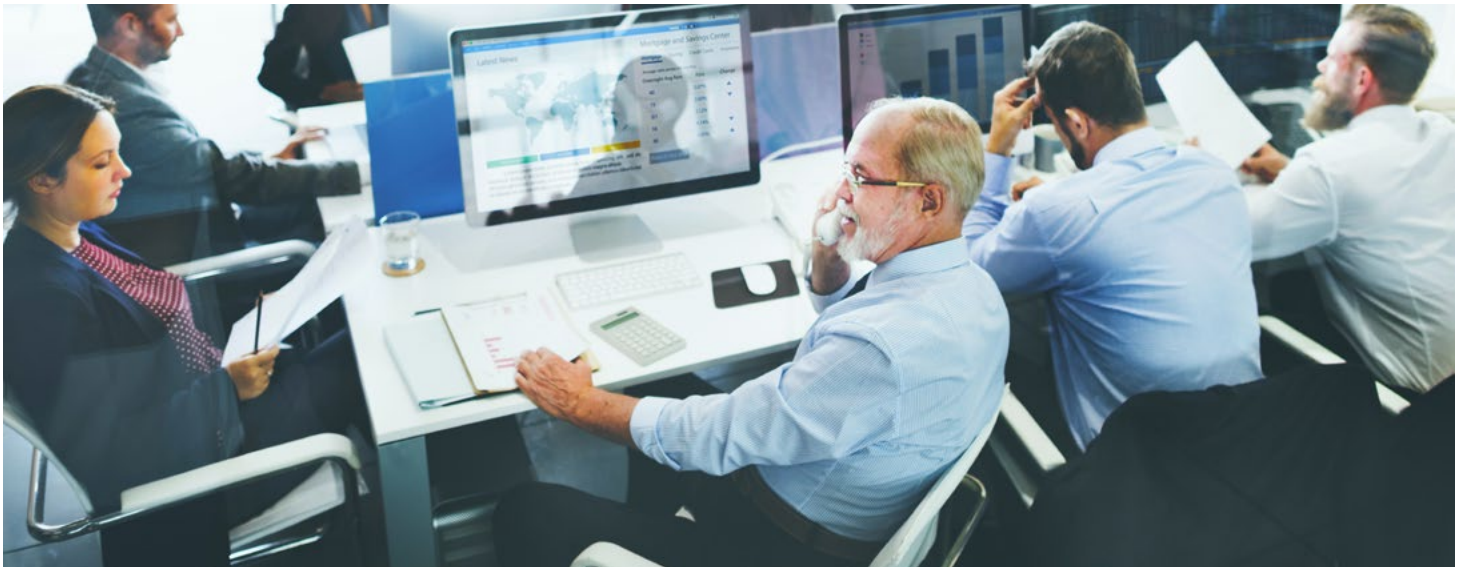
Wat doet u? Oefen regelmatig met het herkennen van verdachte e-mails, telefoontjes en betaalverzoeken. Spreek af bij wie een medewerker twijfels of een mogelijke fout direct meldt.

Waarom is dit belangrijk? Oplichters doen zich bijvoorbeeld voor als uw leverancier, helpdeskmedewerker of als manager binnen uw bedrijf. Zij proberen u een vervalste factuur te laten betalen of inloggegevens te laten delen. Aanvallers gebruiken steeds vaker AI technologie om stemmen en gezichten na te maken. Leer medewerkers dat een overtuigende stem of video geen reden is om een ongebruikelijk verzoek zonder controle uit te voeren.

Wat kunt u zelf doen? Controleer ongebruikelijke, dringende of afwijkende verzoeken via een tweede communicatiekanaal. Deel nooit wachtwoorden of verificatiecodes. Bespreek herkenbare voorbeelden, zoals een leverancier die plotseling een ander rekeningnummer doorgeeft of een manager die opdracht geeft tot een overboeking in verband met een investering of overname. Herhaal dit regelmatig.

Het aanspreekpunt voor meldingen kan u zelf zijn, een vaste collega of uw IT-dienstverlener. Een aparte afdeling is niet nodig. Zorg dat iedereen weet hoe deze persoon te bereiken en meld verdachte situaties snel.

Wat vraagt u aan uw IT-leverancier? 'Hoe melden we een verdachte e-mail of een mogelijk incident? Wie beoordeelt de melding en wat is de vervolgactie? Kunnen jullie helpen met korte, praktische oefeningen?'



8. Spreek af wie verdachte digitale activiteiten controleert

Wat doet u? Laat beveiligingsmeldingen en registraties van activiteiten controleren. Zulke registraties worden logbestanden genoemd. Spreek af wie verdachte inlogpogingen, ongebruikelijke verbindingen en andere afwijkingen beoordeelt.

Waarom is dit belangrijk? Een digitale aanval is niet altijd direct zichtbaar. Controle van activiteiten kan helpen om een overgenomen account of apparaat eerder te ontdekken en de gevolgen te beperken.

Wat kunt u zelf doen? Leg vast wie meldingen ontvangt, wie actie onderneemt en wanneer u wordt geïnformeerd. Vraag om uitleg in begrijpelijke taal. Alleen meldingen verzamelen is niet voldoende: iemand moet ze opvolgen.

Wat vraagt u aan uw IT-leverancier? ‘Welke activiteiten controleren jullie? Zijn waarschuwingen ingesteld voor mislukte inlogpogingen en onverwachte uitbreiding van rechten? Wie reageert op een waarschuwing?’ Laat afhankelijk van uw risico’s beoordelen of centrale analyse van meldingen of extra systemen voor het herkennen en blokkeren van aanvallen nodig zijn.

9. Houd delen van uw netwerk gescheiden

Wat doet u? Laat beoordelen welke apparaten en systemen met elkaar moeten kunnen communiceren. Het opdelen van een netwerk in aparte delen heet netwerksegmentatie. Geef ieder deel alleen de verbindingen die nodig zijn.

Waarom is dit belangrijk? Gescheiden netwerkdelen kunnen het moeilijker maken voor een aanvaller of schadelijke software om zich verder te verspreiden. Zo kunt u belangrijke systemen extra afschermen. Bovendien maakt segmentatie het eenvoudiger om netwerkverkeer te monitoren en afwijkend gedrag te detecteren.

Wat kunt u zelf doen? Overweeg een apart Wifi-gastennetwerk voor bezoekers en een passende scheiding voor verbonden apparaten, zoals camera’s en thermostaten.

Wat vraagt u aan uw IT-leverancier? ‘Is ons gastennetwerk gescheiden van onze bedrijfssystemen? Welke systemen verdienen extra afscherming? Hoe beveiligen we toegang vanaf andere locaties?’ Baseer de keuze op uw apparaten, gegevens, locaties en afhankelijkheden, niet alleen op het aantal medewerkers. Uitgebreide segmentatie is niet voor ieder bedrijf nodig.

10. Maak een noodplan voor digitale incidenten

Wat doet u? Maak een kort noodplan voor een digitaal incident, ook wel een cyberresponsplan genoemd. Leg vast wie beslissingen neemt, wie hulp inschakelt en wie medewerkers, klanten en andere betrokkenen informeert.

Waarom is dit belangrijk? Tijdens een incident moet u vaak snel handelen. Vooraf gemaakte afspraken helpen om overzicht te houden, de schade te beperken en uw werkzaamheden te herstellen.

Wat kunt u zelf doen? Noteer contactpersonen, verantwoordelijkheden en de afspraken over wie u inschakelt als het probleem groter wordt. Leg ook vast hoe uw bedrijf tijdelijk verder werkt en hoe en wanneer medewerkers, klanten, partners of toezichthouders geïnformeerd moeten worden. Oefen het plan regelmatig en werk het bij op basis van de uitkomsten.

Wat vraagt u aan uw IT-leverancier? ‘Wie helpt bij het onderzoeken, beperken en oplossen van een incident? Hoe bereiken we die persoon? Hoe herstellen we systemen en gegevens, en hebben we dat getest?’ Laat eventuele meldverplichtingen afzonderlijk beoordelen en neem de uitkomsten op in uw plan.



Checklist: van inzicht naar actie

Werk de checklist stap voor stap door. De nummers verwijzen naar de tien tips. Noteer per onderdeel de status: geregeld, nog doen of bespreken. Vul ook de verantwoordelijke en de datum in. Hoort een maatregel niet bij uw bedrijf? Noteer dan 'niet van toepassing' en waarom. Werk eerst aan de basis en bespreek technische keuzes met uw IT-leverancier.

A. Basis: zelf regelen of controleren

Tip en basisactie	Status	Wie / datum
1. Beveilig het inloggen. Gebruik unieke wachtwoorden en een wachtwoordkluis. Controleer extra inlogbeveiliging van e-mail, applicaties en bankomgeving. Deel geen wachtwoorden of codes.		
2. Geef alleen toegang die nodig is. Houd rechten bij, verwijder onnodige toegang en spreek af wie software mag installeren. Deel geen accounts of toegangspassen.		
3. Houd software en apparaten up-to-date. Inventariseer systemen, apparaten, applicaties en accounts. Leg vast wie updates verzorgt en welke onderdelen vervangen moeten worden.		
4. Maak en test back-ups. Controleer of belangrijke gegevens worden gekopieerd, wie dat bewaakt en of een recente kopie offline staat. Plan een hersteltest.		
5. Bescherm apparaten en verbindingen. Controleer antivirussoftware en firewalls. Vergrendel apparaten en versleutel vertrouwelijke gegevens.		
6. Maak beveiligingsafspraken met leveranciers. Noteer belangrijke leveranciers en hun toegang. Leg beveiliging en incidentmeldingen vast en houd contactgegevens actueel.		
7. Herken misleiding en meld verdachte situaties. Spreek een meldpunt af, oefen en controleer afwijkende verzoeken via een tweede kanaal. Controleer ook betalingen: stel passende limieten in voor binnenlandse, internationale en batchbetalingen. Verdeel taken en laat waar mogelijk een tweede persoon nieuwe begunstigden en zulke betalingen controleren. Schakel transactiewaarschuwingen in, controleer afschriften en meld verdachte activiteiten direct bij de bank. Blokkeer verloren bankpassen en toegangspassen. Verwijder ongebruikte begunstigden, trek onnodige betaalrechten in, sluit ongebruikte rekeningen en houd contactgegevens actueel.		
8. Spreek af wie verdachte digitale activiteiten controleert. Noteer wie meldingen ontvangt, beoordeelt en opvolgt.		
9. Houd delen van uw netwerk gescheiden. Bespreek een gastennetwerk en inventariseer camera's, thermostaten en andere verbonden apparaten.		
10. Maak een noodplan voor digitale incidenten. Leg contacten, beslissingen, communicatie en herstel vast. Oefen en actualiseer het plan.		

B. Samen met uw IT-leverancier bespreken

Tip en bespreekpunt	Status	Wie / datum
1. Beveilig het inloggen. Controleer extra inlogbeveiliging. Bespreek passkeys, een wachtwoordkluis en veilig herstel van toegang.		
2 Geef alleen toegang die nodig is. Controleer beheerdersrechten en externe toegang. Leg vast wie rechten toekent, beoordeelt en intrekt.		
3. Houd software en apparaten up-to-date. Spreek af hoe updates worden getest, geïnstalleerd en gecontroleerd. Laat oude apparaten veilig wissen voor overdracht of afvoer.		
4. Maak en test reservekopieën. Controleer frequentie en offline opslag. Test volledig herstel en leg volledigheid, bruikbaarheid en afwijkingen vast.		
5. Bescherm apparaten en verbindingen. Controleer antivirussoftware, firewalls en versleuteling bij opslag en verzending. Leg beheer en opvolging vast.		
6. Maak beveiligingsafspraken met leveranciers. Beoordeel beveiliging, toegang en noodplannen. Documenteer bevindingen en meldafspraken. Laat zo nodig juridisch beoordelen welke wettelijke verplichtingen gelden.		
7. Herken misleiding en meld verdachte situaties. Maak meld- en oefenafspraken. Bespreek SPF, DKIM en DMARC: technische maatregelen om e-mailverkeer te beveiligen.		
8. Spreek af wie verdachte digitale activiteiten controleert. Controleer logbestanden. Stel waarschuwingen in voor mislukte inlogpogingen en onverwachte uitbreiding van rechten. Spreek opvolging af.		
9. Houd delen van uw netwerk gescheiden. Controleer scheiding van bezoekers en verbonden apparaten. Bespreek veilige toegang vanaf andere locaties.		
10. Maak een noodplan voor digitale incidenten. Leg hulp bij onderzoek, schadebeperking en herstel vast. Oefen de samenwerking en controleer bereikbaarheid en meldverplichtingen.		

C. Aanvullende maatregelen afhankelijk van uw risico's

Aanvullende maatregel	Status	Wie / datum
Bij tip 2: extra controle in bedrijfssoftware. Bespreek bij uitgebreide administratie-, voorraad- of betalingssystemen registratie van handelingen, verplichte goedkeuringen en scheiding van taken.		
Bij tip 3: onderzoek beveiligingszwaktes. Bespreek kwetsbaarheidsscans en periodieke beveiligingstesten van belangrijke systemen en internetdiensten. Laat een bevoegde specialist beoordelen wat nodig is en volg resultaten op.		
Bij tip 5: aanvullende apparaat- en gegevensbescherming. EDR (Endpoint Detection & Response) helpt verdacht gedrag op apparaten herkennen en opvolgen. DLP (Data Loss Prevention) staat voor maatregelen tegen ongewenste verzending of verlies van gevoelige gegevens. Bespreek of deze nodig zijn.		
Bij tip 5: beveilig geautomatiseerde gegevensuitwisseling. Bespreek bij uitgebreide koppelingen versleutelde verbindingen, beheer van digitale certificaten en digitale ondertekening. Specialisten kunnen PKI-certificaten en HSM's gebruiken voor certificaten en beveiligde opslag van cryptografische sleutels. Controlewaarden van bestanden, oftewel hashwaarden, helpen om wijzigingen te signaleren. Laat werking en beperkingen toelichten.		
Bij tip 8: centrale analyse en herkenning van aanvallen. SIEM (Security Information Event Management) verzamelt en analyseert beveiligingsmeldingen centraal. IDS (Intrusion Detection System) herkent mogelijke aanvallen; IPS (Intrusion Prevention System) kan bepaalde verdachte activiteiten blokkeren. Deze systemen vragen beheer en opvolging en bieden geen volledige bescherming.		
Bij tip 9: verdergaande scheiding en beveiligde toegang. Bespreek aparte netwerkdelen voor belangrijke systemen en veilige toegang op afstand. Een VPN (Virtual Private Network) is een beveiligde verbinding. Zero Trust is een aanpak waarbij toegang niet automatisch wordt vertrouwd, maar passend wordt gecontroleerd. Laat beoordelen wat nodig is.		

ABN AMRO, Bank N.V.
Alle rechten voorbehouden.
2026

Gustav Mahlerlaan 10
1082 PP Amsterdam
Nederland

Kamer van koophandel: 34334259

Disclaimer
Dit document biedt een globaal overzicht van beveiligingsmaatregelen. Dit document is uitsluitend bedoeld voor informatieve doeleinden; er kunnen geen rechten of garanties aan dit document worden ontleend. ABN AMRO heeft bij het samenstellen van dit document redelijke zorgvuldigheid en deskundigheid betracht, maar de informatie in dit document kan mogelijk niet volledig, correct of actueel zijn.

ABN·AMRO